DOI 10.37882/2500-3682.2021.12.17

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧАЩИХСЯ ПРИ ОБУЧЕНИИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ

PROBLEMS OF INFORMATION SECURITY OF STUDENTS' PERSONAL DATA WHEN TEACHING USING DIGITAL EDUCATIONAL PLATFORMS

N. Mironova

Summary: Digital educational environments and platforms, introduced as a supplement and alternative to the traditional format of the educational process, involve the collection, accumulation and processing of arrays of identification and behavioral data about students. Since many of this information is confidential and protected by law, educational platforms should provide an appropriate level of protection for digital personal data, but in practice, the protection of personal data is not always ensured. The article analyzes the problems of using digital educational systems associated with personal data in DSP, their sources; the article outlines the directions of reducing information security risks in the implementation of new education technologies.

Keywords: digital education, digital educational platform, digital educational environment, personal data of students, information security.

Миронова Наталия Геннадьевна
к.ф.н., доцент, ФГБОУ ВО Башкирский государственный университет (Уфа)
om_aks@mail.ru

Аннотация: Цифровые образовательные среды и платформы, внедряемые в качестве дополнения и альтернативы традиционному формату образовательного процесса, предполагают сбор, накопление и обработку массивов идентификационных и поведенческих данных об учащихся. Поскольку многие из этих сведений являются конфиденциальными и охраняются законом, образовательные платформы должны обеспечивать надлежащий уровень защиты цифровых персональных данных (ПДн), но на практике защищенность персональных данных не всегда обеспечивается. В статье проанализированы проблемы использования цифровых образовательных систем (далее ЦОС), связанные с персональными данными в ЦОС, их источники; обозначены направления снижения рисков информационной безопасности при реализации новых технологий образования.

Ключевые слова: цифровое образование, цифровая образовательная платформа, цифровая образовательная среда, персональные данные учащихся, информационная безопасность.

В России реализуются «Стратегия развития информационного общества в РФ на 2017 - 2030 годы», нацпроекты «Цифровая экономика» и «Образование»; их частью является проект создания всероссийской цифровой образовательной среды (далее - ЦОС) (утв. Приказом Министерства просвещения РФ № 649 от 2 декабря 2019 года). Внедрение ЦОС отражает радикальные изменения в модели российского образования. Под экономику данных подстраивается не только правовая среда, корректируются и другие стандарты[1] .

Регламентацию сферы образования сейчас осуществляют разнородный комплекс нормативных документов; упомянет те из них, которые имеют отношение к обработке личные и персональные данные учащихся в цифровых образовательных платформах; 273-ФЗ «Об образовании в Российской Федерации» от 29.07.2012; 44 ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей» от 16.04.2001; ФЗ № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31 июля 2020 г., (ограничивающий применение ФЗ № 152 «о персональных данных» в части безопасности), ФЗ № 123-ФЗ «о внесении изменений в статьи 6 и 10 Федерального закона О персональных данных» от 24 апреля 2020 г.; «Концепция создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

К нормативному регулированию процедур защиты персональных данных учащихся в ЦОС следует отнести 152-ФЗ «О персональных данных», 519-ФЗ «О внесении изменений в ФЗ № 152 о персональных данных» от

1 Например, при проведении он-лайн занятий в дистанционном формате прежние санитарные нормы оказались невыполнимы для образовательных учреждений; - с 1 января 2021 года утверждены новые санитарные правила «Санитарно-эпидемиологические требования к условиям и организациям воспитания и обучения, отдыха и оздоровления детей и молодежи», облегчающие широкое цифровой образовательной среды.

30.12.2020, постановления Правительства РФ («О требованиях к защите ПД при их обработке в ИСПДн», ПП №№ 687, 512, 211). В России действуют правила организации и осуществления государственного контроля и надзора за обработкой персональных данных, существует запрет на использование иностранного ПО для государственных систем (в т.ч. систем обработки ПДн); действуют приказы и методические документы регуляторов в части защиты ПДн (приказы ФСТЭК № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах защиты персональных данных», № 21 от 18.02.2013 о технической защите ИСПДн, приказ (ФСНСС) № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и др.). Так, 519 ФЗ требует активного согласия субъектов ПДн (граждан) на обработку, но согласие теперь означает, что гражданин разрешает вести всю последующую обработку своих ПДн не только структуре, которой он непосредственно разрешил обрабатывать свои личные данные, но и любым «третьими сторонам»; тем самым новый закон «развязал руки» бизнесу в отношении сбор и продажи массивов личных данных граждан, но поставил граждан (например, учащихся в ЦОС) в более уязвимое, чем прежде, положение. В 2021 г. Роскомнадзор в приказе «Об установлении требований к содержанию согласия на обработку ПДн, разрешенных субъектом ПДн для распространения», рекомендовал указывать в соглашении на обработку и использование ПДн, помимо прочего: цель обработки ПДн, категории ПДн, на обработку которых дается согласие, срок, в течение которого действует согласие (но этот срок вряд ли будет соблюдаться оператором, как показывает практика проверить, как фактически используются ПДн после истечения оговоренного срока хранения или отзыв данных для рядового гражданина нереалистично учитывая природу оцифрованной информации и практику работы с базами данных); сведения об информационных ресурсах оператора, дающих доступ неограниченному кругу лиц и иные действия с ПДн. На практике, благодаря системе «безшовных согласий» данные могут без дальнейшего согласия граждан вполне легально утекать в другие системы, с которыми будет интегрирована в перспективе система, и масштаб фактического использования ПДн вряд ли ограничится указанным в Согласии на обработку ПДн. Персональные данные используют для обучения на них систем искусственного интеллекта; для развития технологий ИИ по настоянию IT-компаний пролоббирован ряд законов, которыми вводится «экспериментальный правового режима», отменяющие отдельные ограничения законов о ПДн, чтобы упростить передачу и сбор персональных данных для бизнеса и разработчиков ИИ. Данная практика внесет еще больше рисков безопасности, неподконтрольности оборота персональных данных граждан. Собирая ПДн в системах, действующих в экспериментальном правовом режиме (а к ним относятся и ФГИС ЦОС и т.п. ИС), операторы сбора и хранения ПДн имеют теперь право не сообщать субъекту ПДн цели обработки его данных, не указывать, кто будет оператором обработки ПДн или его представителям, не отчитываться, для чего были собраны и использованы данные; а получившие откуда-либо ПДн граждан в ИС в рамках экспериментального правового режима могут не сообщать кому-либо источники получения ПДн, что дает корпорациям свободу (и безнаказанность) в использования, в т.к. торговле «новой нефтью» (данными о жизни граждан).

Основным контингентом ЦОС являются дети; безопасность детей в информационном пространстве в России регулируют ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и проч. С 2012 году утверждена «Национальная стратегия действий в интересах детей на 2012–2017 годы» (одно из ее направлений – обеспечение информационной безопасности детей). С 2015 по 2020 г. государство в этой сфере руководствовалось положениями «Концепции информационной безопасности детей», осенью 2021 г. проект новой версии «Концепции» на следующий период разработал АНО «Центр изучения и сетевого мониторинга молодёжной среды». Обе концепции критиковались специалистами ИБ за поверхностный и прозападный характер, подмену содержания безопасности детей – медиаграмотностью, неучет ряда цифровых угроз (например, концепция игнорирует проблему вовлечения молодежи в деструктивные течения и т.д.

В тех странах, где образование платное, где учебные заведения не получают поддержки со стороны государства, школы оптимизируют затраты на образование, увольняя учителей и предлагая ученикам учиться с помощью цифровых платформ и он-лайн курсов. В таких странах интернет-платформам достается весь рынок образовательных услуг, а для населения традиционные образовательные инфраструктуры вытесняются цифровым форматом. России, судя по всему, направляется по тому же пути. «Цифровое» лобби подготавливает общественность к новой реальности: «В цифровом мире вуза, существующего в текущем виде, больше не будет. Образовательная система станет сетецентричной экосистемой, в которой образовательные организации трансформируются в провайдеров образовательных сервисов различного размера… Дети, которые будут жить в начале 2020 годов, в принципе, смогут прожить жизнь, ни разу не зайдя в школу и в университет» [3].

Создание он-лайн сервисов (в т.ч. образовательных и около-образовательных) выгодно IT-компаниям, увеличивает их маржинальность, привлекает в лице детей новых клиентов для иных коммерческих сервисов, а также позволяют искать среди обучающихся перспективных специалистов, расширяет общее влияние и конкурентные преимущества IT-компаний в других областях. Ак-

тивный захват рынка образовательных услуг цифровыми компаниями реализует проект по «приватизации» российского образования; бизнес-модель цифровых образовательных платформ и аналогичных проектов во всех странах одинакова: сначала платформа аккумулирует образовательный контент, привлекая учителей и частных разработчиков электронных учебных курсов, сопутствующих сервисов, рекламируя и продвигая платформы как дополнение в школьному, университетскому образованию, а затем начинает действовать как агрессивный конкурент и заместитель традиционных образовательных учреждений; сначала контент предоставляется учащимся или школам бесплатно, а затем – платно. В частности, в странах, где образование платное, школы оптимизируют затраты на образование, увольняя учителей и предлагая ученикам получать «знания» из электронных ресурсов и гаджетов. Образовательным интернет-платформам отводится роль, полностью замещающая традиционные образовательные инфраструктуры.

В России широко используются зарубежные инструменты в образовании: платформы Moodle, Zoom, MS Team, Google Meet, Khan Academy (и ее аналог Interneturok.ru для школьников), образовательную платформу IBLS, OpenEdu, платформы Stepik и Skyeng. Российские платформы оказались менее востребованы [2]; это МЭШ и РЭШ, Moodle, Фоксфорд, «Якласс», СберКласс, Учи.ру, Яндекс.Учебник, mooc.lektorium, Универсариум, системы дистанционного обучения вузов и мало кому известные платформы InternetUrok.ru, «Мои достижения», «Молодые профессионалы», «Ворлдскиллс Россия», «Олимпиум» проч. Сбербанк продвигает проект «СберКласс», Яндекс (владлец - Lastar Trust, Голландия) - платформу «ЯндексШкола». ФГИС ЦОС, МЭШ, РЭШ, «Интернет-школа» от Высшей школы экономики», ресурс «МФТИ Онлайн» реализуются при поддержке госструктур, Источники финансирования большинства образовательных проектов - крупные иностранные IT-компании.

Наблюдается усиление государственно-частного сотрудничества по вопросам образования. Чертой российской бизнес-модели IT-компаний, подвизающихся в области цифрового образования, является их стремление с самого начала выйти на государственные структуры, аффилироваться с региональным или национальными проектом в сфере цифровизации, дабы, используя административный ресурс, бюджетные средства и госзаказы на разработку и продвижение своей IT-продукции, встраивать коммерческие системы в стандартный учебный процесс образовательных учреждений для организации дистанционного взаимодействия учреждения с учащимися; в дельнейшем такая стратегия облегчает замещение традиционной системы образования - цифровой.

С 2001 года в РФ реализовывалась целевая программа «Развитие единой образовательной информационной среды», с 2013 - госпрограмма «Развитие образования» на 2013-2020 гг. (в рамках последней с 2016 г. финансируется проект «Современная цифровая образовательная среда в Российской Федерации» [8]). Эксперимент по использованию цифровой образовательной среды (ЦОС) идет в школах 14 регионов России. Летом 2021 г. начала работа по созданию ФГИС «Моя школа» [6], которая функционируя по всей России, будет интегрироваться с другими ИС через систему СМЭВ и API с Госуслугами, ЕСИА, СМЭВ, с образовательной платформой РЭШ, АИС федерального банка данных о детях без родителей, ГИС о лицах с выдающимися способностями, НСУД, платформой больших данных ЦОС, федеральными и региональными ИС образования, здравоохранения и социального обслуживания и проч.. Среди планируемых функций платформы ФГИС «Моя школа» - мониторинг результатов образовательной деятельности учеников, ведение цифровых профилей и портфолио учеников, формирование индивидуального образовательного маршрута обучения и воспитания, включая профориентацию обучающегося, передачу сведений в ЕСИА, бесшовный переход от сводов информации на ЕПГУ к детальной информации, публикация данных об образовательных событиях (собраниях, контрольных) и проч.

В цифровой формат, помимо обучения, переводятся и другие аспекты образования: аттестаты и дипломы в цифровом виде на сайте госуслуг для выпускников школ на базе МГТУ им. Баумана, СППУ, МПГУ, УрФУ и Российского университета транспорта, далее – по всей стране. Школа в своей цифровой ипостаси становится предприятием по производству не только знаний и компетенций, но и «больших данных» об учащихся. Данные аккумулируются, используются для оптимизации управления.

Обозначив отечественный регуляторный «ландшафт» и средства цифровизации образовательного процесса, перейдем к проблемам информационной безопасности персональных данных (ПДн) учащихся, использующих цифровой формат (ЦОСы, платформы, экосистемы.

За персональными данными охотятся, их ими торгуют и иначе монетизируют. Поведенческие и личные данные граждан привлекают интерес разных категорий потребителей бигдата в разных контекстах. В черной зоне мотивации потребителей ПДн находится фрод (кража финансовой информации идентификационных данных от банковских счетов с целью присвоения денег); кража «цифровой личности» с целью взятия под контроль цифровых ресурсов и физических активов жертвы (например, кража цифровой подписи для переоформления на чужое имя недвижимости и иного имущества); шпионаж. В серой зоне – добыча личных данных методами OSINT и аналитики больших данных для решения управленческих задач (подобные цели в отношении массивов ПДн ставят разведывательные, силовые, фискальные,

политические структуры, рекламный бизнес. К серой зоне отнесем и добычу данных для обучения моделей (например, нейросетей) для решения конкретных задач (поиск и распознавание людей, прогнозирование событий, боевой ИИ и прочее). В «светлой» зоне – агрегирование личных данных граждан (в т.ч. учащихся) в цифровых сервисах ГИС, ИС компаний, банков и страховых компаний, HR-агентств. В частности основными интересантами и спонсорами ЦОС и образовательных платформ стали банки, бизнес и государство, имея в виду получение пользы от доступа к персональным и поведенческим данным. Массивы личных и поведенческих данных планируется использовать для профилирования граждан с разного возраста и моделирования поведения (очевидно, что эти возможности найдут применение не столько в образовательном контексте, сколько в более широком экономическом и политическом управлении). Поведенческий анализ нашел применение для описания и для прогнозирования поведения человека, для управления этим поведением.

Вокруг учащихся, обучающихся в сети большую часть времени, складывается «богатая» экосистема ищущих прямую или косвенную, законную и незаконную выгоду. Но если у обитающей в живой природе особи есть резистентность, врожденные механизмы защиты от опасностей, действующие автоматически, то в цифровой экосистеме, относительно которой у ребенка нет эволюционно обусловленного врожденного инстинкта адаптивного поведения, - в ней подростки беззащитны, поскольку не понимают всего разнообразия рисков. Они не понимают, кого и чего бояться, не знают технических возможностей и мотивов лиц, добывающих сведения с тем или иным умыслом, не понимают для чего и чем защищаться в цифровой среде. Между тем, предоставить всю полноту защиты данных при работе в ЦОС только штатными средствами не получится – уязвимости могут возникать и на любом этапе обмена между точкой доступа к сети - и платформой (все платформы по своей сути стали облачными, обучение происходит дистанционно через сеть с использованием браузера или клиента). При уязвимостях в системе защиты свою выгоду от цифровых образовательных платформ получают и злоумышленники, поэтому ЦОС все чаще становятся объектом кибер-атак; так, по данным Департамента цифровых технологий, культуры, СМИ и спорта США, в 2019 году 80% учреждений дополнительного и высшего образования подверглись кибератакам (или у них были выявлены нарушения кибербезопасности). [1], в России атаки на образовательные системы тоже участились по мере расширения цифровой практики обучения[2] ; массовыми стали атаки кражи учётных данных для доступа к системам аудио- и видеосвязи Skype, Webex и Zoom, где в период эпидемии COVID-19 засветили биометрию своих лиц десятки миллионов людей; осенью 2021 года зафиксирован всплеск DDoS-атак на сайты образовательных учреждений. При этом образовательные цифровые платформы недостаточно защищены от киберугроз[3]. ЦОС могут интересовать злоумышленников для получения идентификационных и поведенческих данных учащихся, зная которые нарушители могут пытаться взломать аккаунты от других сервисов ребенка или его родственников, в т.ч. финансовых[4]. Регистрируясь на ресурсах интернета, подростки оставляют там цифровой след в виде системных и личных поведенческих атрибутов (IP-адрес и ID гаджета или ПК, сведения о операционной системе, номер программного обеспечения, часовой пояс, данные анализа пакетов TCP/IP и SSL/TLS-трафика, cookie-файлы[5] и особенности навигации по web-страницам, идентификационные данные и проч. С устройств можно снять более ста важных атрибутов (время, потраченное на сайте, клики курсора и активность на сайте, изменение настроек системы), трафик браузеров на локальном прокси-сервере. Боты, собирающего цифровые отпечатки, стоят в даркнет недорого для хакера (5-200 долларов) [9]; скопировав параметры с браузера и другие персональные характеристики жертвы, злоумышленник может от ее имени красть аккаунты для продажи, мошенничества, шантажа, рассылки спама, создавать бот-нет сетей для организации DOS-атак на другие ресурсы; «кража личности» (подкладывание в свой браузер чужого цифрового отпечатка) позволяет ему выполнять незаконные действия от имени жертвы, обманывать антифрод-системы банков и другие сервисов). Чувствительная категория данных – биометрические и медицинские данные о человеке, его близких (например, получив эти сведения, банки и страховые могут менять тактику в отношении своих клиентов, а кадровики и злоумышленики могут сильно осложнить человеку в будущем жизнь, а хекеры могут использовать для взлома систем с биометрическим способом аутентификации, совершения преступлений и т.п.). Другие пути потери контроля учащихся за своими персональными данными – фишинг (подмена легальных сайтов-платформ сайтами-имитациями обучающих платформ и сервисов видеоконференций для кражи ошибочно вве-

2 пример: частая проблема, с которой столкнулись участники учебных онлайн-конференций в 2020-21 гг., – посторонние пользователи, срывавшие занятия разными техническими способами самой платформы, - т.н. zoombombing

3 Например, такое мнение высказывает аналитики компании StormWall, которая специализируется на защите онлайн-ресурсов от кибератак (см. «В начале учебного года сфера образования серьезно пострадала от DDoS-атак URL: https://safe.cnews.ru/news/line/2021-10-15_v_nachale_uchebnogo_goda_sfera (дата публикации: 15.10.2021))

4 многие дети сейчас имеют интернет-кошельки и т.н. «детские карты»

5 Куки-файлы – текстовые файлы на компьютерах пользователей, содержащие сведения о предыдущих действиях на сайтах.

денных регистрационных данных (Лаборатория Касперского засвидетельствовала [7] инциденты такого рода с 170 000 потерпевшими пользователям лишь за весну 2020 года. Утечки личных данных возникают по вине инсайдеров информационных сервисов и систем, из-за кражи путем взлома системы защиты, с помощью шпионского программного обеспечения, из-за незащищенности мобильных и домашних смарт-устройств, с которых пользователь посещает интернет, из-за «бэкдоров» (и иных уязвимостей), оставленных разработчиками в приложениях, из-за использования open-source средств разработки (например, API-инструментария, облегчающего злоумышленникам кражу и взлом), из-за широкого использования смарт-устройств и цифровых ассистентов. (Согласно исследованию компании InfoWatch, лишь в 2020 г. около 100 млн. записей личных данных россиян, включая биометрию, утекли в открытый доступ; по оценкам экспертов, российские компании и банки скрывают 57% утечек данных. [4])

Для частных образовательных платформ требования по защите персональных данных проще, чем для ГИС ИСПД (в отличие от ГИС, коммерческим учебным системам нет обязательной аттестации, нет необходимости защищать ИСПД наложенными сертифицированными средствами защиты[6], нет и требований по обязательной сертификации коммерческой системы на отсутствие недекларированных возможностей, которые вообще-то могут оказаться в любом сегмента сети, включающей ИСПД (в приложениях узлов, веб-серверов, операционных систем, в сетевом и периферийном оборудовании, подключенном к сети). Это означает, что коммерческие образовательные платформы на практике могут быть более уязвимы к угрозам ИБ в отношении ПДн, чем государственные образовательные системы, платформы. Разработчик или вендор цифрового сервиса, под давлением требований законов и контроля регуляторов в сфере информационной безопасности, на словах заверяет субъектов ПДн в безопасности предоставленных персональных данных, но на практике эта безопасность может быть не реализована по вине как разработчика или оператора персональных данных, так и по виде внешних причин.

Чем больше личных данных собирает цифровая платформы, тем привлекательнее она для злоумышленников и тем тяжелее потенциальный ущерб субъекту персональных данных в случае их утечки и незаконного использования. Сложившейся практикой стал сбор сайтами и платформами избыточной личной информации о пользователях, сбор и обработки таких данных не связана с необходимостью выполнения основной функции платформ, но они их собирают, редко уделяя внимание надлежащей защите. Пример: ФГИС ЦОС, чья функция для пользователей – образовательная, намерена собирать такие сведения об учащемся в ЦОС [5]: помимо ФИО, даты рождения, сведений об образовании, ученой степени и звании обучающегося, о профессиональной переподготовке и (или) повышении квалификации, почты и телефона (что уже привычно требуют образовательные ресурсы с пользователя), - также планируется хранить явно избыточные для получения образования, но несущие много рисков для человека в случае утечки, персональные сведения (п. 24): «о трудовой деятельности (включая работу по совместительству, предпринимательскую и иную деятельность), военной службе; о государственных наградах, иных наградах и знаках отличия; адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; реквизиты страхового свидетельства обязательного пенсионного страхования; идентификационный номер налогоплательщика», причем хранится в системе они будут пожизненно – «не меньше сроков хранения информации, которые устанавливаются для хранения документов в бумажном виде, содержащих такую информацию». Но за это время с системой и ее обладателями могут произойти разные трансформации - система может поменять собственника и стать частной, причем с иностранными владельцами (как это часто случается с IT-ресурсами в России), систему будут обновлять, интегрировать со все большим числом информационных систем, - но вопросы использования в будущем третьими сторонами персональных данных учащихся не затронуты в положении о ГИС ЦОС) В Положении ГИС ЦОС [5] определено, что она будет обмениваться данными (в т.ч. ПДн учащихся и преподавателей) с иными ИС и образовательными платформами: порталом «Госуслуги»; ЕСИА; ФГИС «Единая система нормативной справочной информации»; порталом информационной и методической поддержки инклюзивного высшего образования; иными образовательными платформами, базами данных и информационные системы (п. 26 Постановления). - Т.о., перечень иных операторов, имеющих легальный доступ к ПДн учащихся ГИС ЦОС, обширен и будет пополняться, значит, риски утечки и нецелевого использования личных данных учащихся, «бесшовно» передаваемые через многочисленных операторов и инсайдеров указанных систем, многократно повышаются. Также, в документе ничего не сказано о том, что будет с персональными данными учащихся после вывода ЦИС из эксплуатации или модернизации, если ЦОС изменит своей правовой или функциональный статус.

Для снижения рисков ПДн нередко обезличивают,

6 Гусейнов Р. Аналитическая записка о соответствии программной платформы «Первая Форма» требованиям нормативно-правовых актов Российской Федерации в области безопасности персональных данных // Сайт компании «Первая форма». URL: https://1forma.ru/personal-information.html#_ftn19

чтобы усложнить их вредоносное использование (методы обезличивания описаны, например, в «Требованиях и методах по обезличиванию персональных данных» (утв. Приказом Роскомнадзора от 5 сентября 2013 г. № 996) (впрочем и по обезличенных данным в ряде случае можно идентифицировать человека, которого они характеризуют). Для снижения рисков НСД и утечки ПДн применяются средства защиты с технологией DNS-фильтрации для локальных сетей образовательных учреждений - но новый формат обучения учащихся планируется реализовывать из дома, но защитить такой обширный образовательный периметр никакая концепция или система защиты не в состоянии и не по карману ученикам. Сейчас биометрическая и многофакторная аутентификация считается более надежным способом ограничения доступа к защищаемой системе, но это удорожит всю систему и не является панацеей от угроз несанкционированного доступа.

Актуальной угрозой для цифровых образовательных систем является потеря доступности дистанционного предоставляемых ресурсов; причем угроза мало связана с совершенством системы защиты самих ЦОС, поскольку разрыв связи учащегося с платформой при удаленном доступе может случиться по множеству причин, - и студент и преподаватель остается наедине с самим собой. Я наблюдаю эту проблему повсеместно: разработчики или операторы услуги, когда нужно решить проблему недоступности ресурса для учащегося или преподавателя на практике физически недоступны, проблема с отсутствием доступа к системе не решается неделями, - пока это не станет критично для самого оператора). Я это наблюдаю на практике при работе в вузовских образовательных платформах и образовательных платформ государственно-частного толка (типа Иннополиса и проч.), несмотря на то, что на словах и «на бумаге» все превосходно и должно работать. Пока проблемы касаются лишь отдельных учащихся или конкретной организации, и есть альтернативы. Но логика развития рынка и IT-решений в сторону олигополизации и монополизации сервисов цифровых услуг такова, что в ближайшей перспективе владельцем цифровой образовательной услуги будет какой-то один субъект, и отключенными от образовательной цифровой системы могут оказаться целые сегменты сети и регионы, но достучаться до кого-то где-то там на том конце сети окажется невозможно для маленького клиента большой цифровой корпорации (учащийся просто останется наедине со своей проблемой в глухой деревне или большом городе).

Да и способно ли дать цифровое образование какие-либо навыки, кроме тех, которые могут быть оцифрованы (на сегодня оцифрованы лишь навыки, связанные с пассивным восприятием контента, виртуальной игрой, или сводятся к генерации текстов; но к ним ведь не сводится реальная практика выживания и реальная экономика, для которой образование в первую очередь должно готовить кадры). Даже математика как навык делать, а не использовать готовые средства, осваивается не в цифровой среде, а в реальности, на бумаге, – сужу, об этом, будучи математиком. Традиционные формы образовательного процесса являются и средством формирования реальных социальных навыков учащихся, которые многогранны (в т.ч. осваивать социальные роли в меняющемся социальном окружении (что формирует структуру личности), трезво воспринимать критику, слышать и понимать чужое мнение и вырабатывать свое, понимать людей и сотрудничать с ними при выполнении сложной деятельности разного характер, разумно решать конфликты; скудная цифровая виртуальная среда не дают этих возможности во всей полноте)

Задачи владельцев образовательных платформ утилитарны (главным образом, максимизация прибыли); если решение о выборе контента и управлении образовательной траекторией учащегося принимает алгоритм или нейросеть (как нам обещают разработчики ЦОС) – это решение надо верифицировать и корректировать по человеческим меркам; в системе образования этим заняты сегодня десятки тысяч людей; если из заменит автоматика, какова будет социальная цена технологических ошибок?

Традиционное образование помимо познавательной функции выполняло и функции социализации (и более широкой адаптации будущего члена общества к выживанию в естественной среде обитания), ребенок взаимодействовал в образовательной среде с людьми разного возраста, разного опыта, а сидящий в виртуальной среде платформы «маугли», изолированный от людей и приспособленный к машине, приобретет черты того, с чем контактирует, от чего усваивает картину мира и нормы поведения. Чем будет общество людей, разделенных с детских лет стенами в своих виртуальных «образовательных пузырях» цифровых платформ, движимых по индивидуальным траекториям искусственным интеллектом и незримыми менторами, - страшно представить…

Сейчас много пишут и говорят о том, что от цифрового формата получения образования обществу эпохи «экономики данных» не уйти (да и много усилий и финансов уже вложено). Значит, разработчикам, образовательным субъектам, людям-субъектам персональных данных, государству, придется предпринимать продуманные усилия, чтобы цифровая прозрачность и большие данные не несли вреда безопасности частной и общественной жизни сегодняшних детей – завтрашних граждан, которые будут определять жизнь страны, российского общества. В этом направлении (а не в лоббируемом IT-компаниями) должно развиваться законодательство в сфере информационной безопасности. А учащиеся должны научиться понимать информационные рисках и приобрести навы-

ки «выживания» в среде сетевых сервисов. Разработчики должны больше, чем это практикуется, внимания и ответственности проявлять в вопросах именно безопасности при проектировании и разработке образовательных систем, а операторы, вендоры и специалисты по защите должны находится под более жестким, чем сейчас, контролем со стороны государства, чтобы практиковали ответственное и вдумчивое отношение к сбору, хранению и защите массивов личной информации граждан, и чтобы игры разработчиков и IT-бизнеса с «большими данными» не вылились для страны в большую проблему национальной безопасности. Также желательно формировать более справедливую и «симметричную» для субъектов информационного права - правовую среду в России, в которой граждане не выступали бы лишь в роли объекта контроля, регулирования со стороны государственных и бизнес-структур, и источника информации (как бесправная новая нефть), а имели право на защиту и ограничение сбора личной информации о себе, и реальную возможность контролировать дальнейшее использование своей личной информации.

ЛИТЕРАТУРА

1. Бродская М. Это Cyber EdTech, детки! Новые технологии на защите старых образовательных подходов // BIS Journal. № 2(41). 2021. https://ib-bank.ru/bisjournal/post/1612 (Дата публикации: 13 июля 2021)
2. Ильина Н., Виноградова Е. Защита отечественных: экосистемам хотят возмещать ущерб в случае санкций // Известия. URL: https://iz.ru/1264419/natalia-ilina-ekaterina-vinogradova/zashchita-otechestvennykh-ekosistemam-khotiat-vozmeshchat-ushcherb-v-sluchae-sanktcii (Дата публикации: 15 декабря 2021)
3. Концепция «Единая цифровая образовательная экосистема» / команда экспертов ИТ-компании IBS. 2019. URL: https://www.ibs.ru/media/media/kontseptsiya-edinaya-tsifrovayaobrazovatelnaya-ekosistema
4. Миронова Н.Г. Методы антиспуфинга в системах биометрической идентификации и верификации // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 21-22 мая 2021 года) / отв. ред. А.С. Исмагилова Уфа: РИЦ БГУ, 2021. – 282 с. – С. 43-52. URL: https://www.elibrary.ru/item.asp?id=47220569
5. Положение о ГИС «Современная цифровая образовательная среда», утв. постановлением Правительства РФ от 16 ноября 2020 г. № 1836. URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102910737&page=1&rdk=0&intelsearch=%CE+%CF%C5%D0%D1%CE%CD%C0%CB%DC%CD%DB%D5+%C4%C0%CD%CD%DB%D5++&link_id=188#I0
6. Приказ Министерства просвещения РФ и от 30 июня 2021 г. N 396 О создании федеральной ГИС «Моя школа».
7. Сиденко А. Прогнозы в сфере образования на 2021 год // Kaspersky security bulletin. URL: https://securelist.ru/education-predictions-2021/99470 (03 декабря 2020)
8. Современная цифровая образовательная среда в РФ. URL: http://neorusedu.ru/about (дата обращения: 1.12.2021).
9. Lakshmanan R. 120 Compromised Ad Servers Target Millions of Internet Users // hehackernews.com URL: https://thehackernews.com/2021/04/120-compromised-ad-servers-target.html (April 20, 2021)

Журнал «Современная наука: актуальные проблемы теории и практики»